DoD 5200.1-M

DEPARTMENT OF DEFENSE

ACQUISITION SYSTEMS PROTECTION PROGRAM

MARCH 1994

THE ASSISTANT SECRETARY OF DEFENSE FOR COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-3040

COMMAND, CONTROL, COMMUNICATIONS AND INTELLIGENCE

March 16, 1994

FOREWORD

This Manual is issued under the authority of DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982. The protection standards and guidance described within this Manual are required to prevent foreign intelligence collection and unauthorized disclosure of essential program information, technologies and/or systems during the DoD acquisition process. The goal of the program is to selectively and effectively apply security countermeasures to protect essential information, reduce costs, and reduce administrative burden of security.

This Manual applies to the Office of the Secretary of Defense (OSD), the Military Departments, the Chairman of the Joint Chiefs of Staff, the Unified Combatant Commands, the Inspector General of the Department of Defense (IG, DoD), the Defense Agencies, and the DoD Field Activities (hereafter referred to collectively as "the DoD Components").

This Manual is effective immediately and it is mandatory for use by all of the DoD Components and for incorporation into those DoD contracts where it is required. No supplementation of the requirements of this Manual is required; however, the Heads of the DoD Components may issue supplementary instructions when necessary to provide for unique requirements within their DoD Components. Any additional guidance issued by the DoD Components shall be forwarded to Deputy Assistant Secretary of Defense (Intelligence and Security) (DASD(I&S)), within 6 months of implementation and after each subsequent change.

Send recommended changes to the Manual through channels to:

Assistant Secretary of Defense for Command, Control,
Communications and Intelligence
Office of the Deputy Assistant Secretary of Defense
(Intelligence and Security), OASD(C3I)
6000 Defense Pentagon
Washington, DC 20301-6000

The DoD Components may obtain copies of this Manual through their own publication channels. Approved for public release; distribution unlimited. Authorized registered users may obtain copies of this publication from the Defense Technical Information Center, Cameron Station, Alexandria, VA 22304-6145. Other Federal Agencies and the public may obtain copies from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, Virginia 22161.

Emmett Paige, Jr.

TABLE OF CONTENTS

REFERENCES

(a) DoD Directive 5000.1, "Defense Acquisition," February 23, 1991

(b) JCS Pub 1-02, "Department of Defense Dictionary of Military and Associated Terms," December 1, 1989

(c) DoD 5200.1-R, "Information Security Program Regulation," June 1986, authorized by DoD Directive 5200.1, June 7, 1982

(d) Public Law 96-72, "The Export Administration Act of 1979," September 29, 1979 as amended (50 U.S.C. 2401 et seq.) by Public Law 97-145, "The Export Administration Act of 1981," December 29, 1981; Public Law 99-64, "The Export Administration Amendments Act of 1985," July 12, 1985; and Public Law 100-418, "The Multilateral Export Control Enhancement Amendments Act," August 23, 1988

(e) DoD Directive 2040.2, "International Transfer of Technology, Goods, Services, and Munitions," January 17, 1984

(f) DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982

(g) DoD Instruction 5000.2, "Defense Acquisition Management Policies and Procedures," February 23, 1991

(h) DoD 5400.7-R, "Department of Defense Freedom of Information Act Program," October 1990, authorized by DoD Directive 5400.7, May 13, 1988.

(i) Executive Order 12356, "National Security Information," June 23, 1982

(j) DoD Directive 8120.1, "Life-Cycle Management (LCM) of Automated Information Systems (AISs)," January 14, 1993

(k) DoD Instruction 8120.2, "Automated Information System (AIS) Life-Cycle Management (LCM) Process, Review, and Milestone Approval Procedures," January 14, 1993

(l) DoD Directive 5230.11, "Disclosure of Classified Military Information to Foreign Governments and International Organizations," June 16, 1992

(m) DoD Directive 5230.20, "Visits and Assignments of Foreign Representatives," April 24, 1992

(n) "Intelligence Collection Capabilities Matrix (U)," Defense Intelligence Agency, DIW-2400-731-93, March 1993, SECRET/NOFORN

(o) "Foreign Interest in U.S. Critical Technologies Matrix (U)," Defense Intelligence Agency, PC-1830-14-93, November 1993, SECRET/NOFORN/WINTEL/NOCONTRACT

(p) DoD Instruction 5240.4, "Reporting of Counterintelligence and Criminal Violations," September 22, 1992

(q) DoD Directive 5525.7, "Implementation of Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes," January 22, 1985

(r) DoD 5220.22-M, "Industrial Security Manual for Safeguarding Classified Information," January 1991, authorized by DoD Directive 5220.22, December 8, 1980

(s) DoD 5200.1-H, "Department of Defense Handbook for Writing Security Classification Guidance," March 1986, authorized by DoD Directive 5200.1, June 7, 1982

(t) DoD Directive 5230.24, "Distribution Statements on Technical Documents," March 18, 1987

(u) DoD Directive 5230.25, "Withholding of Unclassified Technical Data from Public Disclosure," November 6, 1984

(v) DoD 5200.1-I, "Index of Security Classification Guides," August 1992, authorized by DoD Directive 5200.1, June 7, 1982

(w) DoD Directive 5530.3, "International Agreements," June 11, 1987

(x) Military Standard 1785, "System Security Engineering Program Management Requirements," September 1, 1989

(y) DoD Directive 5200.8, "Security of DoD Installations and Resources," April 25, 1991

(z) DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

(aa) DoD Directive C-5200.5, "Communications Security (COMSEC) (U)," April 21, 1990

(bb) DoD Directive C-5200.19, "Control of Compromising Emanations (U)," February 23, 1990

(cc) DoD 5220.22-R, "Industrial Security Regulation," December 1985, authorized by DoD Directive 5220.22, December 8, 1980

(dd) DoD 5200.2-R, "DoD Personnel Security Program," January 1987, authorized by DoD Directive 5200.2, May 6, 1992

(ee) DoD 5200.8-R, "DoD Physical Security Program," May 1991, authorized by DoD Directive 5200.8, April 25, 1991

(ff) AR 55-355/NAVSUPINST 4600.70/AFR 75-2/MCO P4600.14B/DLAR 4500.3, "Defense Traffic Management Regulation," July 31, 1986

(gg) DoD Directive 5240.2, "DoD Counterintelligence," June 6, 1983

(hh) DoD Directive 5205.2, "DoD Operations Security Program," July 7, 1983

DEFINITIONS

1. Acquisition Facilities. DoD facilities primarily involved in activities related to research, development of systems, testing, or evaluation of test results.

2. Acquisition Systems Protection (ASP). The safeguarding of defense systems anywhere in the acquisition process as defined in DoD Directive 5000.1 (reference (a)), the defense technologies being developed that could lead to weapon or defense systems, and defense research data. ASP integrates all security disciplines, counterintelligence, and other defensive methods to deny foreign collection efforts and prevent unauthorized disclosure to deliver to our forces uncompromised combat effectiveness over the life expectancy of the system.

3. Adversary. An individual, group, organization, or government that must be denied essential information.

4. Component Intelligence (Counterintelligence) Analysis Centers. Within this Manual, the organizations of the DoD Components that produce the Multi-Discipline Counter-intelligence (MDCI) Threat Assessments for use in program protection planning. In some DoD Components, these organizations are labeled as intelligence organizations, while in others they are part of counterintelligence organizations.

5. Compromise. The known or suspected exposure of EPITS or classified information or material to persons who are not authorized access.

6. Counterintelligence. Those activities intended to detect, counteract, and/or prevent espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations conducted by or on behalf of foreign powers, organizations or persons; it does not include personnel, physical, document, or communications security programs.

7. Counterintelligence and Security Countermeasures (CI/SCM) Support Element. The organizational elements that provide staff-level functional support to program managers in the areas of counterintelligence, security programs and countermeasures, or operations security.

8. Countermeasures. That form of military science that by employment of devices and/or techniques has as its objective the impairment of the operational effectiveness of enemy activity (JCS Pub 1-02, reference (b)). Countermeasures may include anything that effectively negates an adversary's ability to exploit vulnerabilities.

9. Delegation of Disclosure Authority Letter (DDL). A letter required as part of the Technology Assessment/Control Plan, prepared by the cognizant DoD Component, that provides detailed guidance regarding releasibility of all elements of the system or technology in question. The DDL must be approved by Under Secretary of Defense for Policy (USD(P)) before any promise or release of sensitive technology.

10. Essential Program Information, Technologies, and/or Systems (EPITS). That information about the program, technologies, and/or systems that if compromised would degrade combat effectiveness or shorten the expected combat-effective life of the system. Access to this information could

allow someone to kill, counter or clone the acquisition system before or near scheduled deployment or force a major design change to maintain the same level of effectiveness.

11. Foreign Intelligence Collection Threat. The potential of a foreign power, organization, or person to overtly or covertly collect information about U.S. acquisition program technologies, capabilities, and methods of employment that could be used to develop a similar weapon system or countermeasures to the U.S. system or related operations.

12. Infrastructure. Those items that are used by more than one acquisition program in the pursuit of the development of defense systems. The infrastructure includes laboratories, test facilities, the policy and procedure structure, and education and training organizations.

13. Matrix Support Element. (See definition 7., above, Counter-intelligence and Security Countermeasures (CI/SCM) Support Element.)

14. Milestone Decision Authority The individual designated in accordance with criteria established by the Under Secretary of Defense for Acquisition and Technology to approve entry of an acquisition program into the next phase of the acquisition process.

15. Multi-Discipline Counterintelligence (MDCI) Threat Assessment. An assessment made by the cognizant DoD Component that describes those foreign governments, entities, or activities that have the interest and capability to collect information about a system under development.

16. Operations Security (OPSEC) A process of analyzing friendly actions attendant to military operations and other activities to:

a. Identify those actions that can be observed by adversary intelligence systems.

b. Determine the indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation.

17. Program Information. For the purposes of this program, information that includes programmatic data and/or information and weapons system, subsystem, or component information.

18. Program Protection. The safeguarding of defense systems and technical data anywhere in the acquisition process to include the technologies being developed, the support systems (e.g., test and simulation equipment), and research data with military applications. This protection activity involves integrating all security disciplines, counterintelligence, and other defensive methods to protect the essential program information, technologies, and systems data from intelligence collection and unauthorized disclosure.

19. Program Protection Inspection. An inspection, conducted at a defense contractor facility, to assess compliance with the contractually imposed countermeasures requirements developed by the program

protection planning process. These inspections will normally be conducted by the Defense Investigative Service as part of its periodic industrial security inspections of the facility.

20. Program Protection Plan (PPP). A comprehensive protection and technology control management plan established for each defense acquisition program to identify and protect classified and other sensitive information from foreign intelligence collection or unauthorized disclosure. (The PPP is designed to negate the Program Protection Threats and Vulnerabilities.)

21. Program Protection Survey. A survey, conducted during each acquisition phase, to assess the effectiveness of the countermeasures prescribed in the program protection plan at a specific point in time.

22. Program Protection Threats The program protection threats include life-cycle protection threats, foreign intelligence collection efforts, and unauthorized disclosure of essential program information, technologies, and systems during the acquisition process.

23. Risk Management. The comparison and analysis of the relative threat (intent and capability to collect the information); the vulnerability of the asset; the cost and administrative burden of possible countermeasures; and the value of the asset used to determine the appropriate level of protection to control and reduce the risk of compromise or disclosure to acceptable levels. Risk management allows the acceptance of risk in the security process based upon a cost-benefit analysis.

24. Sensitive Information. Any information, the loss, misuse, or unauthorized access to which would or could adversely affect the organizational and/or national interest but which does not meet classification criteria specified in DoD 5200.1-R (reference (c)).

25. Special Access Program. Any program imposing need-to-know or access controls beyond those normally provided for access to Confidential, Secret, or Top Secret information. Examples of such controls include, but are not limited to, special clearance, adjudication, or investigative requirements; special designation of officials authorized to determine need to know; or special lists of persons determined to have a need-to-know.

26. System Decomposition. The separation of the major mission functions and capabilities of the system and then identifying those components or technologies that give the system this ability.

27. System Security Engineering (SSE). An element of system engineering that applies scientific and engineering principles to identify and reduce system susceptibility to damage, compromise, or destruction; the identification, evaluation, and elimination or containment of system vulnerabilities to known or postulated security threats in the operational environment.

28. System Security Management Plan. A formal document that fully describes the planned security tasks required to meet system security engineering requirements, including organizational responsibilities, methods of accomplishment, milestones, depth of effort, and integration with other program engineering, design and management activities, and related systems.

29. System Threat. The threat to be countered by the defense system being acquired.

30. System Threat Assessment Report (STAR). The basic authoritative threat assessment, tailored for and focused on, a particular (i.e., single) U.S. major defense system. It describes the threat to be countered in the projected threat environment. The threat information should reference DIA-validated documents.

31. Technology

a. The information and know-how (whether in tangible form, such as models, prototypes, drawings, sketches, diagrams, blueprints, or manuals, or in intangible form, such as training or technical services) that can be used to design, produce, manufacture, utilize, or reconstruct goods, including computer software and technical data, but not the goods themselves. (Export Administration Act of 1979, as amended in 1981, 1985 and 1988, reference (d))

b. The technical information and know-how that can be used to design, produce, manufacture, use, or reconstruct goods, including technical data and computer software. The term does not include the goods themselves. (DoD Directive 2040.2, reference (e))

32. Technology Assessment/ Control Plan (TA/CP). The document that identifies and describes sensitive program information; the risks involved in foreign access to the information; the participation in the program or foreign sales of the resulting system; and the development of access controls and protective measures as necessary to protect the U.S. technological or operational advantage represented by the system.

33. Technology Transfer Transferring, exporting, or disclosing defense articles, defense service, or defense technical data covered by the U.S. Munitions List to any foreign person or entity in the United States or abroad.

34. Threat. The sum of the potential strengths, capabilities, and strategic objectives of any adversary that can limit or negate U.S. mission accomplishment or reduce force, system, or equipment effectiveness. (See definition 22., above, Program Protection Threats.)

35. Time- or Event-Phased Classification Guide. The adaptation of the DoD security classification guide to the acquisition process addressing the essential program information, technologies, or systems and the associated subsystems and technologies during each phase of the acquisition process. The guide indicates classification or sensitivity and the date or event that will cause a change to the level of the classification or sensitivity.

36. Vulnerability. The susceptibility of systems or components to the threat in a given environment.

ABBREVIATIONS AND ACRONYMS

ACAT	Acquisition Category
AFOSI	Air Force Office of Special Investigations
AIS	automated information system
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ASP	Acquisition Systems Protection
ASPO	Acquisition Systems Protection Office
CDRL	Contract Data Requirements List
CI	counterintelligence
COMSEC	communications security
CONUS	continental United States
DAB	Defense Acquisition Board
DASD(I&S)	Deputy Assistant Secretary of Defense for Intelligence and Security
DDL	Delegation of Disclosure Authority Letter
DESA	Defense Evaluation and Support Agency
DIA	Defense Intelligence Agency
DID	Data Item Description
DIS	Defense Investigative Service
DISP	Defense Industrial Security Program
DoD	Department of Defense
DSN	Defense Switched Network
EEFI	Essential Elements of Friendly Information
EPITS	Essential Program Information, Technologies, and/or Systems
FOUO	For Official Use Only
HUMINT	human intelligence
IG, DoD	Inspector General of the Department of Defense
IOC	Initial Operational Capability
ISM	Industrial Security Manual
MDCI	Multi-Discipline Counterintelligence
MNS	Mission Needs Statement
MRTFB	Major Range and Test Facility Base
NISP	National Industrial Security Program
NDP	National Disclosure Policy
NOCONTRACT	Not Releasable to Contractors and/or Consultants

OASD(C3I)	Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence
OPR	office of primary responsibility
OPSEC	operations security
ORCON	Dissemination and Extraction of Information Controlled by Originator
OT&E	operational test and evaluation
OUSD(A&T)	Office of the Under Secretary of Defense for Acquisition and Technology
PEO	program executive officer
PM	program manager (also project or product manager)
POC	point of contact
PPP	Program Protection Plan
PPS	Program Protection Survey
PROPIN	Proprietary Information Involved
R&D	Research and Development
RDT&E	Research, Development, Test and Evaluation
S&T	Science and Technology, or Science and Technical
SAP	Special Access Program
SEMP	System Engineering Management Plan
SOT	Subsystem or Technology
SSE	System Security Engineering
SSEM	System Security Engineering Manager
SSMP	System Security Management Plan
STAR	System Threat Assessment Report
STU	secure telephone unit
TA/CP	Technology Assessment/Control Plan
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USD(P)	Under Secretary of Defense for Policy
WRM	Wartime Reserve Mode

CHAPTER 1

GENERAL INFORMATION

A. PURPOSE

1. In accordance with DoD Directive 5200.1 (reference (f)), and DoD Instruction 5000.2 (reference (g)), and DoD 5400.7-R reference (h)), this Manual prescribes standards, criteria, and methodology for the identification and protection of DoD Essential Program Information, Technologies, and/or Systems (EPITS) within DoD acquisition programs. Any additional guidance issued by the DoD Components to implement the requirements contained in this Manual shall be furnished to the DASD(I) within 6 months of the date of this Manual or following the issuance of additional guidance.

2. The standards and criteria in this Manual are intended to protect against loss and unauthorized disclosure of EPITS throughout the acquisition process at all involved locations or facilities. They will also identify and reduce projected operational system susceptibility to damage, compromise, or destruction.

3. The ultimate goal is to selectively and effectively apply security countermeasures to protect the EPITS and reduce costs by applying risk management.

B. SCOPE

1. This Manual applies to all DoD Components that are involved in the acquisition of DoD systems in accordance with DoD Directive 5000.1 (reference (a)), in providing security support to DoD or DoD contractor facilities, and in the DoD intelligence and/or counterintelligence programs.

2. This Manual does not apply to acquisitions by DoD Components that involve Special Access Programs created under the authority of Executive Order 12356 (reference (i)) or acquisition of Automated Information Systems under DoD Directive 8120.1 (reference (j)) and DoD Instruction 8120.2 (reference (k)); however, to the extent feasible and appropriate, DoD Components should adhere to the program protection planning provisions provided in this Manual for those acquisition programs. Before Special Access Programs transition to collateral status, the requirements of this Manual shall be met.

3. The Manual defines the processes by which information, technologies, and systems that are essential to the successful development and deployment of new DoD systems are identified and protected.

4. EPITS covered by this Manual shall be identified, prioritized, and protected in accordance with the program protection plans (PPPs) prescribed in this Manual.

5. The criteria in the Manual shall be applied at all locations where EPITS are analyzed, maintained, stored, used, developed, transported, or produced.

C. RESPONSIBILITIES

1. The Under Secretary of Defense for Acquisition and Technology (USD(A&T)) shall:

a. Delegate to the ASD(C3I), the responsibility to

review the PPP for each Acquisition Category (ACAT) 1D program as part of the Defense Acquisition Board (DAB). Consider the results of the review for inclusion in the Acquisition Decision Memorandum as appropriate.

b. Delegate to the Director, Special Programs, the responsibility to ensure that for programs defined as "Highly Sensitive Classified Programs," in accordance with DoD Directive 5000.1 (reference (a)), that PPPs are prepared to ensure that EPITS are properly protected when the programs transition from special access to regular classified requirements.

c. Assist with the development of a horizontal protection system for technology and information by requiring the identification of EPITS for all acquisition programs, products, technology demonstrators,and other acquisition activities that have been designated for incorporation into, or support of, another acquisition program, and ensure that appropriate OUSD(A&T) staff elements coordinate the transfer of information between program offices.

2. The Under Secretary of Defense for Policy (USD(P)) shall support program protection efforts by:

a. Ensuring that acquisition special access programs, international security agreements, and co-production efforts adhere to overall systems protection requirements.

b. Sharing information in the Security Policy automated databases with the Acquisition Systems Protection (ASP) community.

c. Providing standard DoD-wide automation support to the Acquisition Systems Protection System to include support for the horizontal protection and assessment program in accordance with responsibilities assigned in this Manual and DoD Directive 5230.11 (reference (l)), DoD Directive 2040.2 (reference (e)), and DoD Directive 5230.20 (reference (m))).

d. Making or approving, as applicable, and monitoring necessary security arrangements with other governments.

3. The Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I)) shall:

a. Assist the USD(A&T) by reviewing the PPP for each DAB-level acquisition program and providing a report of the evaluation to the appropriate DAB committee.

b. Conduct horizontal protection activities to ensure the commonality of protective measures for similar essential DoD information, to measure effectiveness of efforts and to support national-level protection activities.

c. Serve as the DoD focal point for contact with government agencies outside of the DoD that provide assistance in protecting DoD EPITS.

4. The Inspector General, DoD, shall undertake compliance inspections of selected programs.

5. The Heads of the DoD Components shall:

a. Ensure that all acquisition programs are protected in accordance with this Manual and DoD Instruction 5000.2 (reference (g)).

b. Direct the appropriate staff office to review each

Acquisition Category (ACAT) ID acquisition program to determine that the PPP has been prepared and is adequate before submitting the plan to OSD as part of the acquisition milestone review.

c. Direct the review of each acquisition program in ACAT IC, II, III, and IV by the appropriate Milestone Decision Authority (MDA) to determine that the PPP is adequate as defined by the exit criteria listed in Appendix A.

d. Ensure contracts involving the protection of EPITS at contractor facilities describe the standards of protection to be provided, in accordance with the developed and approved PPP.

e. Ensure, by contractual clause, access to prime and subcontractor facilities to enable the Government to conduct surveys, inspections, and investigations as necessary to ensure the successful implementation of program protection activities.

f. Provide intelligence threat assessment support required for each acquisition program managed by the Component.

6. The Director, Defense Intelligence Agency (DIA), shall:

a. Provide a periodic written report detailing the intelligence collection capabilities of all foreign entities deemed as possible threats to the DoD systems in the acquisition process.

b. Provide periodic reports (references (n) and (o)) contrasting, in each critical technology area, the market forecast of competitive countries with U.S. technology efforts. The report should relate this information to the list of DoD critical technologies. In addition, include in the report the forecast of the military technology needs of the threat countries. Include technologies regardless of their being on the list of DoD critical or key technologies.

c. Update these reports periodically, as determined by a prioritized listing of threat countries.

d. Perform technology transfer risk assessments for foreign countries of concern and foreign intelligence threat assessments in support of DoD-wide ASP planning.

7. The Director, Defense Investigative Service (DIS), shall:

a. Assist, as necessary, with program protection surveys at defense contractor facilities in the United States by helping with the selection or modification of appropriate security countermeasures necessary to prevent foreign intelligence collection and unauthorized disclosure of EPITS not protected by the Defense (National) Industrial Security Program (DISP/NISP).

b. Conduct inspections of contractor facilities within the United States to assess compliance with program protection countermeasures, including those for the protection of sensitive unclassified information, when contract provisions authorize such inspections.

c. Assess contract compliance when security requirements and DIS or Federal entry authority, as required by paragraph C.5.e., are contractually established.

D. INFORMATION REQUIREMENTS

1. The reporting requirements contained in section C.6.a. and b. of this Manual have been assigned Report Control Symbol DD-C3I(TRI)-1937.

2. Incidents of loss, compromise, or theft of identified EPITS or other classified information should be reported in accordance with the procedures in DoD Instruction 5240.4 (reference (p)) and DoD Directive 5200.1 (reference (f)).

CHAPTER 2

POLICY

A. GENERAL

1. The DoD Components shall apply appropriate resources to acquisitions systems protection programs at all levels to provide cost-effective protection for each defense acquisition program.

2. Sensitive information and technologies shall be identified early in each acquisition program and protected from inadvertent or unauthorized disclosure as required by subsection B.5. of Part 1 of DoD Directive 5000.1 (reference (a)).

3. The appropriate, Component-level, intelligence and threat analysis center shall prepare a multi-discipline threat assessment addressing the foreign intelligence collection threat and the potential impact upon the combat effectiveness of the program resulting from disclosure of EPITS for each acquisition program as required by DoD Instruction 5000.2 (reference (g)).

4. A comprehensive protection and technology control program shall be established for each defense acquisition program. This effort shall identify and protect classified and other sensitive information concerning that program as required by DoD Instruction 5000.2, Part 5, Section F (reference (g)). This comprehensive protection and technology control plan is known as the program protection plan (PPP).

5. Some acquisition programs may not contain any EPITS as defined by this Manual. If a program manager (or designated representative) complies with the requirements of this Manual for the identification of EPITS and subsequently determines that no EPITS exist within the program (either organic or inherited from supporting programs), then an abbreviated PPP may be prepared. The abbreviated PPP shall be a statement (signed by the program manager) that EPITS, as defined in this Manual, do not exist. Also, the statement shall state the security classification guide has been reviewed and appropriate time or event phasing has been integrated. Once completed, this abbreviated PPP shall be approved by the Program Executive Officer (PEO). Further, it shall be included in the document review in preparation for a milestone decision by the MDA.

6. A PPP shall be prepared for each acquisition program, in accordance with DoD Instruction 5000.2, Part 5, Section F (reference (g)). The plan shall address the following areas: (These areas shall be discussed and updated at each acquisition milestone decision point.)

a. System Description and Elements to be Protected (EPITS),

b. Protection Threats and Vulnerabilities,

c. Countermeasures Concept, and

d. Protection Costs.

7. Program protection plans shall include as attachments the time- and event-phased security classification guide, and, when applicable, the Technology Assessment and Control Plan

(TA/CP) and Delegation of Disclosure Authority Letter (DDL) after foreign access, participation, or sales are authorized. The acquisition systems protection effort should be compatible with and be supported by the system security engineering program (DoD Instruction 5000.2, Part 6, Section J (reference (g)). A summary of the System Security Engineering (SSE) plan shall be attached to the PPP at milestone II.

8. Review and approval of PPPs shall be performed as part of the DoD acquisition milestone decision process. OUSD(A&T), with the support of OASD(C3I), is responsible for the review of the protection programs planned for Acquisition Category (ACAT) ID programs, and the Milestone Decision Authorities are responsible for directing the review of the protection programs planned for all other acquisition programs. Although the program manager is the approving authority for the PPP, the reviewer shall direct changes in the PPP to correct deficiencies.

9. For all ACAT ID programs, the PPP is reviewed by the Acquisition Systems Protection Office in the Office of the Secretary of Defense. For ACAT IC, II, III, and IV programs, the review of the PPPs will be conducted as directed by the Component Acquisition Executive.

10. If a program or product is a component or subsystem of another program, then its protection plan is subject to review by the same review authority as its supported program. Any shortcomings or deficiencies identified in this review are the responsibility of the preparing office and shall be corrected by that office immediately.

11. Disclosures of classified information to and participation by foreign persons in DoD acquisition programs shall be governed by DoD Directive 5230.11 (reference (l)) and DoD Directive 5230.20 (reference (m)).

12. The acquisition chain of command may direct the use of the PPP format for any activity, including science and technology programs, automated information systems, or advanced technology demonstrators to ensure the protection of critical technology from known or suspected threats.

B. ACQUISITION SYSTEMS PROTECTION AND SYSTEM SECURITY ENGINEERING

Acquisition Systems Protection is the overall concept of protecting the program's EPITS from compromise and inadvertent loss from the establishment of the Mission Needs Statement (MNS) to demilitarization. As a minimum, the PPP is developed to protect the program during the period from the development of the MNS until the system is fielded (Initial Operational Capability (IOC)), and through any modification period that may require protection from compromise. System Security Engineering (SSE) is an engineering program directed at negating the threats to completed, deployed systems while the systems are in an operational environment. SSE achieves this objective by incorporating design features directly into the systems to reduce the costs and burdens of security operations after deployment.

C. SUPPORTING AND SUPPORTED PROGRAMS

Managers of acquisition programs and other activities designated to support or be incorporated into other acquisition programs have special responsibilities with regards to

acquisition systems protection. This includes the following:

1. Any activity (e.g., program or project office) that produces technology, information, or systems for another acquisition program shall identify the Essential Program Information, Technologies, and/or Systems (EPITS) (see definition 10.) of which its product is composed to the supported program office.

2. Unresponsive supporting programs shall be identified to the appropriate decision authority by the supported program office.

D. INTELLIGENCE ANALYSIS

The identification of the collection threat to the acquisition program shall be the responsibility of the Component Intelligence Analysis Center of the acquiring DoD Component. The PEO will be responsible for providing matrix support assets to the program office to assist with the analysis of the intelligence product.

1. For joint programs, the lead Component shall be responsible for coordinating the production of the intelligence threat documentation.

2. The DoD goal for the return of a complete Multi-Discipline Counterintelligence (MDCI) threat assessment is 120 days from receipt of the request at the appropriate intelligence production center.

3. To facilitate the preparation of an initial draft PPP, the local support office for counterintelligence and/or security countermeasures (CI/SCM) should furnish a generic, summarized collection threat assessment (based upon the DIA Intelligence Collection Capabilities Matrix (reference (n))and Foreign Interest in U.S. Critical Technologies Matrix (reference (o))) within 30 days of the request to the requesting program office. This initial draft will be used in the initial planning and draft of the PPP. Final drafts of the PPP shall not be prepared by the program office or agent thereof, until the final MDCI analysis is returned to the program office.

E. INTELLIGENCE SUPPORT PROGRAMS

For those activities whose primary objective is the collection and dissemination of intelligence information or technical data on foreign weapon systems, the following special provisions apply:

1. If the activity or program is not subject to the review process of DoD Instruction 5000.2 (reference (g)), the information produced and procedures used shall be protected in accordance with DoD 5200.1-R (reference (c)).

2. If the activity is governed by DoD Instruction 5000.2 (reference (g)), but collects the information purely by passive means, then the information produced and procedures used shall be protected in accordance with DoD 5200.1-R (reference (c)).

3. If the program procures equipment (foreign or domestic) and conducts a formal test and evaluation program, then a PPP should be prepared and implemented, unless the equipment is part of a weapon system that is itself covered by a separate PPP.

F. ACQUISITION PROGRAMS VERSUS ACQUISITION SYSTEMS

1. Throughout this Manual, the terms "acquisition program" and "acquisition system" are used often. However, these two terms are not synonymous and are not to be used interchangeably.

2. The term acquisition program refers to the specific development program being managed under a single program manager. It includes all of the activities that are conducted to define, develop, test, and produce a defense system.

3. The term acquisition system refers to the weapon or defense system being developed and fielded by the acquisition program. It also includes all logistics support equipment, training simulators, test equipment, and other support items that are required to successfully deploy the defense system to its intended operating environment.

G. PROGRAM PROTECTION SURVEYS

1. Program Protection Surveys (PPSs) are conducted following the establishment and integration of PPPs. The PPS is the primary tool of the Program Manager (PM) in evaluating and validating the currently planned protection methodologies. The PPS is focused on specific, valid threat and countermeasures issues. PPS reports from a team requested by a PM are the property of the PM, and further distribution of the unsanitized version is neither required nor authorized.

2. PPSs are not punitive and shall be used only to identify strengths and weaknesses in current program protection planning.

3. Should evidence of criminal activity be discovered during a PPS, the activity shall be reported through appropriate DoD Component channels and acted upon under applicable DoD Component guidance, and referred for any appropriate action under DoD Directive 5525.7 (reference (q)).

4. Upon receipt of a completed PPS report, the PM shall produce a lessons learned document with the assistance of the surveying team. The lessons learned document should not contain any reference to specific locations or programs. Its focus is the effective or ineffective use of the program's established countermeasures to known or suspected vulnerabilities and the identification of unrecognized vulnerabilities. This sanitized version shall be forwarded through the DoD Components to DASD(I) to assist with refinements to the ASP process.

H. HORIZONTAL PROTECTION

1. A Horizontal Protection Program shall be established within the DoD Components to ensure that EPITS are adequately and uniformly protected within the Component.

2. The Horizontal Protection Program ensures that DoD acquisition programs developing new or revised program protection plans have access through a standard DoD-wide automated system, centrally maintained by OUSD(P), to databases comprised of lists of EPITS identified by other DoD acquisition programs and the protective levels and measures being planned. Access to the database allows the programs to compare levels of classification and sensitivity.

3. EPITS that have already been identified by one DoD Component shall be provided similar protection in acquisition programs of all DoD Components. If a conflict develops in the appropriateness of planned protective measures for a particular EPITS, the issue will be resolved at the lowest level review authority common to both programs. The decision of the review authority should be based upon the principle of risk management not risk avoidance.

I. TRAINING

1. The DoD Components responsible for acquisition programs shall establish training programs for those personnel responsible for the preparation and execution of PPPs.

2. The DoD Components shall ensure that periodic refresher training is conducted for all personnel responsible for the protection requirements set forth in program protection planning documents. This training will include the current threats and the design of effective countermeasures.

J. WAIVERS AND EXCEPTIONS

1. No authority has been granted to the DoD Components to waive or exempt this protection planning requirement.

2. The level of detail and complexity in the PPP may vary in accordance with the criticality of the system and its EPITS, and the phase of the acquisition process being addressed.

K. SPECIAL ACCESS PROGRAMS (SAPs)

SAPs, due to their unique nature, have security policies and procedures that (in the aggregate) meet the goals and requirements of this Manual. However, SAP program managers shall develop plans for the protection of the acquisition program as it transitions to general or unclassified status. Such plans should be comprehensive and minimize the disruption to the protection measures during the transition. The program office should meet all requirements of this Manual before it is removed from SAP provisions.

CHAPTER 3

PROGRAM PROTECTION PLANNING

A. GENERAL

Program protection is the safeguarding of a defense system's EPITS anywhere in the acquisition process. This includes technologies being developed, support systems (e.g., test and simulation equipment), and basic research data with military applications. To realize the objectives of program protection, the following actions are part of the program protection planning process that shall be conducted for each DoD acquisition program.

1. Identify and set priorities on those operational or design characteristics of the system that make it unique and provide superior mission capabilities.

2. Identify the system EPITS.

3. Identify specific program locations where the system EPITS are stored, used, developed or analyzed.

4. Identify the intelligence collection threat to the program.

5. Identify the program's vulnerabilities to specific threats at specific locations during each phase of the acquisition cycle.

6. Identify the time- or event-phased countermeasures to be employed by the PM to reduce, control or eliminate specific vulnerabilities of the program and commit the program to a minimum level of protection for EPITS.

7. Identify the protection costs associated with the personnel, products, services, equipment or other areas used as part of program protection planning, the countermeasures or program protection surveys.

8. Identify elements that require classification, when and how long such control should be used. (These activities are discussed in Chapter 4.)

9. Identify the risks and benefits of developing, producing, or selling the system abroad, as well as the methods used to protect the EPITS if such an arrangement is authorized, and whether an export variant is necessary. (These activities are discussed in Chapter 5.)

10. Identify the design features or support equipment required to reduce operational security vulnerabilities upon deployment. (These activities are discussed in Chapter 6.)

B. COORDINATION

1. Although the PM bears the responsibility for the development and implementation of the PPP, close coordination with several staff elements within and external to the program office is essential.

a. The PM should ensure the close cooperation between the security, foreign disclosure, and technical staffs in the development of the PPP. As a result, the PM should seek the advice and assistance of individuals who can:

(1) Evaluate and describe the value of the technology or system in terms of military capability or technology superiority.

(2) Identify foreign availability of like or similar systems and technology.

(3) Describe the threat.

(4) Conduct a risk versus gain analysis when foreign access, participation or sales are recommended.

(5) Perform a "functional decomposition" of the system, whereby the major functions and capabilities are identified and matched to technology or information that gives these components those traits.

(6) Identify any unique fabrication or manufacturing processes necessary to duplicate the technology by an adversary.

(7) Define the criteria for the "loss" of the essential element. The PM should consult with individuals who know the industrial and scientific capabilities of the threat nations to determine if they can use or sell the essential element.

(8) Assist with the preparation of the intelligence request and interpretation of the Multi-Discipline Counter-intelligence (MDCI) analysis prepared by the Component-level intelligence center.

(9) Serve as the primary liaison between the program office, intelligence agencies, counterintelligence organizations, local and Federal law enforcement agencies, and security specialists.

b. Not all program offices will have trained personnel who can perform all of these tasks. As a result, PMs should consult the appropriate staff in the matrix support element for assistance with some of these tasks.

c. One or more matrix support elements may provide support to each program manager in the specialty areas of security countermeasures, operations security, counterintelligence, and intelligence. These matrix support elements, referred to as the counterintelligence and/or security countermeasures (CI/SCM) matrix support elements, serve as the primary liaison between the program office and both intelligence and counterintelligence agencies, as well as other security organizations; for example, security staffs and law enforcement.

2. PMs shall brief the PPP to their program executive officer (PEO) before each milestone review as part of the document review process. In addition, each time a formal assessment of the plan is conducted or the PM elects to change the countermeasures due to a change in the EPITS, threat, or environment, the PM and PEO must mutually agree to any proposed changes. Results of assessments that reveal criminal activity, fraud, waste, or abuse, or threats to National Security should be reported through appropriate channels. Otherwise, results of any assessment should not be released to any activity outside the program office without the written authorization of the PM.

3. PMs shall ensure that the developing agency identifies and places in priority sequence the EPITS for any component, subsystem, technology demonstrator, or other research program being developed by an independent activity that is planned for incorporation into the PM's program. Further, the PM of the program using this technology shall ensure the inclusion of the subsystem's EPITS in the PPP of the incorporating program.

a. The parent program manager shall ensure the sub-

element's EPITS are protected at least at an equivalent level as they are protected in the sub-element's program.

b. The PMs of systems that incorporate subsystems that have not identified the EPITS shall direct the office that developed the technology to supply this information. For those supporting activities that are defined as acquisition programs in accordance with DoD Directive 5000.1 (reference (a)) and that have failed to develop a PPP, the PM of the program that will incorporate the technology in question may direct the developing program office to provide an approved PPP.

4. The purpose of these coordination activities is to ensure the PPP that is developed and implemented is effective, focuses on the essential elements of the program, minimizes costs and administrative burdens, and avoids duplication of effort.

5. The protection of an acquisition program's EPITS should be revised by the DoD Component when a recognized shortcoming exists in the PPP.

C. PROGRAM PROTECTION PLAN

1. The PPP for an acquisition program should serve as the single source document used to coordinate and integrate all of the protection efforts designed to deny foreign collection activities and prevent inadvertent disclosure.

a. The PPP for an acquisition program shall be established and approved by the PM as soon as possible after the validation of the Mission Needs Statement. As a minimum, the PPP shall be prepared and subject to review by the Milestone Decision Authority (MDA) (or designated representative) during the Milestone I Review or the first review after Milestone 0. The results of the review shall be considered by the MDA for inclusion in the Acquisition Decision Memorandum.

b. The scope of the PPP should address, as necessary, the entire life cycle of the acquisition program from the date the plan is established until demilitarization.

2. The preparation and implementation of the PPP for an acquisition program relies on risk management, not risk avoidance. The costs associated with the protection of the system's EPITS shall be balanced against the costs of protection and potential impact of the loss or compromise of the EPITS.

3. In accordance with DoD Instruction 5000.2, Part 5, Section F, (reference (g)), the PPP is a required document for all acquisition programs.

a. Any programs, products, technology demonstrators, or other items developed as part of a separate acquisition process that are components or subsystems of the program shall have their PPP reviewed by the parent program's Milestone Decision Authority during the supported program's Milestone Review.

b. The effectiveness of the PPP is highly dependent upon the quality and currency of the information available to the program office.

(1) Coordination between the program office and the CI/SCM matrix support element is critical to ensure any changes in the system's EPITS, threat, or environmental conditions reach the proper organizations.

(2) Intelligence and counterintelligence organizations

that support the program protection effort are encouraged to supply information on foreign activities to the program offices without waiting for periodic production requests once they have received the initial list of the program's EPITS.

4. The PPP should be classified if the content of the plan dictates.

5. The DoD Components do not need to mandate a specific format for PPPs. However, each PPP shall address the following items:

a. System Description.

b. Program Information.

c. Essential Program Information, Technology, and/or Systems.

d. Vulnerabilities to Intelligence Collection.

e. Foreign Intelligence Collection Threat.

f. Time-Phased Plan of Protection (Countermeasures).

g. Cost of Protection.

h. Time- or Event-Phased Security Classification Guide.

i. Technology Assessment Control Plan.

j. System Security Engineering Approach (Milestone II and later).

6. Specific guidance on the topics to be addressed in the PPP is given in sections D. through J. below.

D. SYSTEM DESCRIPTION

Since most acquisition programs combine existing, proven technology and information with new, state-of-the-art technology, the system description should provide the reviewer with a clear indication of the capabilities and limitations of the system being acquired, including support equipment, simulators, and other supporting equipment. The system description shall discuss:

1. The anticipated battlefield employment of the system.

2. The strategic, operational, or tactical impact of the system's development and deployment.

3. The specific characteristics that distinguish it from existing systems or other systems under development.

4. The function, operational characteristics, and technical parameters of any component program, product, technology demonstrator, or other acquisition system that is an integral part of the system.

E. PROGRAM INFORMATION

The program information shall discuss the organization and structure of the office responsible for developing and fielding the acquisition system. The program description should briefly describe the following:

1. The acquisition chain of command for the program, including the Milestone Decision Authority for the program and sub-programs.

2. The location, points of contact, and telephone number of the government-owned sites that will handle, store, or analyze EPITS-related material.

3. The location, point of contact, and telephone number of government-owned test and evaluation centers where EPITS-related material will be tested.

4. The corporation name, location, point(s) of contact, and telephone number of primary contractors who handle or have access to EPITS-related materials.

5. The location, point(s) of contact, and telephone number of contractor-owned facilities, other than those identified in subsection E.4. above, where EPITS-related materials will be tested. These locations may include subcontractors, vendors, or other non-government locations.

F. ESSENTIAL PROGRAM INFORMATION, TECHNOLOGIES, AND/OR SYSTEMS (EPITS)

The EPITS of the system are the critical elements of the system that make it unique and valuable to U.S. defense forces. The EPITS are those items that, if compromised, would cause a degradation of combat effectiveness, decrease the combat-effective lifetime, or allow a foreign activity to clone, kill, or neutralize the U.S. system. They are those pieces of information or technology that provide the essential capability that must be protected. As such, the EPITS are the foundation upon which all protection efforts for the program are based.

1. The EPITS are components, engineering, design or manufacturing processes, and technologies; system capabilities and vulnerabilities and other information that give the system its unique capability on the battlefield or limit the ability of other countries to reproduce the essential capabilities or mission.

2. To develop the EPITS, the PM (or representative) and the system engineer perform a "functional decomposition."

a. This process starts with the system description and then identifies those specific components or attributes that give the system its unique ability.

b. A similar analysis is performed on each subassembly or component until a specific piece of technology or equipment can be associated with each sub-task that gives the overall system its ability on the battlefield.

c. Once these components are isolated, the PM should evaluate their potential as EPITS by applying the following four questions:

(1) If a foreign intelligence service or other entity obtained this item, could they determine a method to kill the U.S. system?

(2) If a foreign intelligence service or other entity obtained this item, could they determine a method to degrade or neutralize the U.S. system?

(3) If a foreign intelligence service or other entity obtained this item, could they determine a method to clone the U.S. system?

(4) If a foreign intelligence service or other entity obtained this information, would the U.S. system need major modifications to maintain its strategic or tactical advantage for the system's projected operational lifetime?

d. An affirmative answer to any of these questions would qualify the item as an EPITS or a component of an EPITS. A component of an EPITS is known as a Subsystem or Technology (SOT).

3. In addition to the elements organic to the system, the PM shall consider any engineering process, fabrication technique, diagnostic equipment, simulators, or other support equipment associated with

the system for consideration as a possible EPITS. Special emphasis should be placed on any process that is unique to the system under development. The PM and program engineer should evaluate each of these areas and identify any activity unique to the United States industrial and technology base that limits the ability of foreign nations to reproduce or counter the system.

4. Once the PM has reduced the EPITS list, further refinement is necessary.

a. To assist the intelligence analysts with their task of identifying the collection threats to the system, the PM, with the help of the matrix support elements, should describe the EPITS in terms used by one of the various technology control lists (e.g., The Militarily Critical Technologies List or the National Disclosure Policy category). The fact that a particular technology is listed in one of the technology control lists does not necessarily mean that the technology is an EPITS for a system.

b. Specific guidance should be provided on the criteria for "loss" or compromise.

c. The PM should indicate whether the element is a Treaty-Limited Item under the provisions of one of the arms control treaties.

d. A discussion of the use of this EPITS by any other acquisition program or on any other system should be indicated.

e. The list of EPITS should be prioritized to ensure that the most important information is emphasized during analysis of the protection costs. The CI/SCM matrix support elements and the DoD Component ASP coordinator should be able to help the PM complete this task.

G. VULNERABILITIES

1. Vulnerabilities are the susceptibility of the program to the threat(s) in a given environment.

2. The vulnerabilities possessed by the program's EPITS shall be based upon:

a. How the EPITS are stored, maintained, or transmitted (e.g., electronic media, blueprints, training materials, facsimile, or modem).

b. How the EPITS are used (e.g., bench testing or field testing).

c. What emanations, exploitable signals, or signatures (electronic or acoustic) are generated by the EPITS or reveal them (e.g., telemetry, acoustic, or radiant energy).

d. Where the EPITS are located (e.g., program office, test site, contractor, or vendor).

e. What types of OPSEC indicators or observables are generated by program or system functions, actions, and operations involving EPITS.

3. Once the vulnerabilities are identified, the PM shall place them in priority sequence order.

a. The sequence should be based upon the consequences of the loss or compromise of the EPITS that are involved.

b. Factors that should be considered include the impact upon the combat effectiveness of the system, the effect on the combat-effective lifetime, the cost associated with any modification required to compensate for the

loss, and the choice of alternatives (such as the technology used or the test range used) that are available.

H. FOREIGN INTELLIGENCE COLLECTION THREAT

1. A threat exists when a foreign government or entity has a confirmed or assessed requirement for the acquisition of classified or sensitive defense information, or proprietary commercial information; the capability exists to acquire such information; and the acquisition of the information by the foreign entity would be detrimental to U.S. interests.

a. Confirmed or assessed identification of foreign requirements will provide indications of the most probable sources and methods that a foreign government or entity might employ to satisfy a collection requirement.

b. For the purposes of this Manual, a threat requires the combination of an EPITS-related item with a known or suspected vulnerability, a known collection capability and somebody with the interest or intention to collect the information.

2. The intelligence collection threat data used by the program office shall be based upon a National-level intelligence estimate.

a. This estimate is known as a Multi-Discipline Counterintelligence (MDCI) threat assessment and it is supplied by the appropriate DoD Component counterintelligence analysis center.

b. The MDCI analysis is not based on the threat described in the System Threat Analysis Report (STAR). The STAR describes the battlefield threat the system will be designed to face. The MDCI analysis is directed at those governments, entities, or activities that have the interest and capability to collect information about the system under development. However, sudden changes in the anticipated operational threat should be reviewed as they occur to determine (if possible) if the change is due to successful intelligence collection.

c. The PM and the matrix support element shall compare the results of the MDCI threat assessment with the EPITS and vulnerabilities to determine the level of risk to the program.

d. The program team should integrate into the MDCI threat assessment those environmental factors that might assist or reduce the ability of the foreign intelligence service to collect information at a given location.

3. The counterintelligence centers shall base their MDCI threat assessment upon the compiled list of EPITS and their potential vulnerabilities, which are submitted by the program office. As a result, the MDCI threat assessment shall, as a minimum, answer the following questions about the EPITS (within the constraints of existing intelligence information and the need for a prompt and timely reply):

a. Have any of the EPITS been compromised or lost (as defined by the program office), by either overt or covert means?

b. Which countries or organizations have an interest in the EPITS and, if known, why?

c. What capabilities do each of these countries or organizations have to collect intelligence information on the

EPITS at each location identified by the program office?

4. The appropriate CI/SCM matrix support element should assist the program office in preparing the intelligence production request to the appropriate DoD Component counterintelligence analysis center.

a. The matrix support elements should expedite the request to the intelligence center that would normally support the PEO from the program's lead DoD Component.

b. An additional copy should be sent to the intelligence analysis center of any other DoD Component involved in the program (for information only) to facilitate a single, unified position on the collection threat.

5. The intelligence production request should contain the following information (as determined necessary by the appropriate DoD Component) before its submission to the counterintelligence analysis center:

a. Program office name, designator, and address.

b. PM's name and telephone number.

c. Matrix support element point of contact's name, address, and telephone number.

d. Supporting or supported programs' or products' names, locations, and telephone numbers.

e. Operational employment role.

f. Loss or compromise criteria.

g. Relationship to key technologies or other controlled technology lists of the Department of Defense or Department of Commerce.

h. Distinguishing traits or emissions; methods of EPITS transmittal, usage, storage, testing; etc.

i. Use of foreign equipment or technology during testing (if possible).

j. Anticipated foreign involvement in the development or production of the system.

k. Contractor names, locations, points of contact, and telephone numbers, as well as the identification of each EPITS at each location.

6. After the intelligence production request is completed, the matrix support element should provide a generic, summarized collection threat assessment to the program office within 30 days.

a. This assessment should be based upon the Defense Intelligence Agency's collection capability and technology threat matrices (references (n) and (o)).

b. This initial assessment will only provide an indication of which countries have the capability to collect intelligence on the system and the possible interest or intention to collect it.

c. This assessment is not unique to the program or system.

d. This assessment may serve as the basis of an initial draft of the PPP.

e. A draft PPP shall not be submitted by the program office for approval until a copy of the final MDCI threat assessment is returned from the Military Department or DoD

Component intelligence analysis center and the results incorporated into the PPP, unless the Service fails to provide the MDCI analysis within the timelines established by this Manual.

7. While awaiting the return of the MDCI threat assessment, the matrix support element should compile and prepare the local collection threat supplement with the assistance of the supporting counterintelligence organization. Any local threat information collected as part of this process should be sent expeditiously through channels to the Component-level Intelligence Analysis Center for validation and possible inclusion in the final MDCI product.

8. The MDCI threat assessment prepared by the Component-level, intelligence analysis center should be returned to the appropriate matrix support element as soon as possible. The goal is to return the complete, MDCI threat assessment within 120 days of the receipt by the counterintelligence analysis center.

9. The MDCI threat assessment should clearly indicate specific information that may not be released to contractors.

a. Since contractors play a critical role in the success of the Acquisition Systems Protection effort, the use of handling restrictions and distribution statements such as NOCONTRACT (Not Releasable to Contractors /Consultants), ORCON (Dissemination and Extraction of Information Controlled by Originator), and PROPIN (Caution - Proprietary Information Involved), DoD 5220.22-M (reference (r)), should be minimized by the organization preparing the MDCI threat assessment.

b. In the event such restrictions are placed on the MDCI threat assessment, a collateral version of the MDCI analysis that is releasable to contractors should be prepared and returned to the matrix support element concurrently with the original MDCI threat assessment.

I. COUNTERMEASURES CONCEPT

The countermeasures concept is a statement of the overall approach for applying countermeasures to eliminate or reduce the projected vulnerabilities of each EPITS. The countermeasures include anything which effectively negates an adversary's ability to exploit vulnerabilities.

1. Countermeasures should only be developed to eliminate vulnerabilities associated with an identified threat to the EPITS based upon the MDCI analysis.

a. The countermeasures developed shall be time- or event-phased.

b. The countermeasures shall not be implemented until they are required, and they shall be terminated or reduced as soon as possible after the threat, EPITS, or environmental changes lead to a reduction or elimination of the vulnerabilities or negation of the threat.

2. PMs should establish a countermeasures program based upon a cost-benefit analysis.

a. The analysis should focus on the cost associated with the deployment of the appropriate countermeasure compared to the risk associated with loss or compromise of the essential element.

b. The cost-benefit analysis prepared by the program office is for internal use only. It is not required as an enclosure,

It is not required as an enclosure, annex, or chapter of the PPP as part of the approval process.

c. The PM should discuss and justify in the countermeasures section of the PPP why any recognized EPITS vulnerabilities do not have countermeasures developed to reduce, control, or eliminate them.

3. Should the acquisition program not have an assigned or contracted security apparatus, the appropriate matrix support elements should help the program office develop a draft countermeasures concept, based upon the PM's guidance and intent.

4. The establishment of a protection baseline is the goal of the countermeasures concept section.

a. There should be a commitment to a level of protection to ensure protection of the EPITS.

b. The minimum level of effort and cost should be applied to guarantee a level of protection appropriate to the PM's final estimate of the intelligence collection threat to the system.

5. The DoD Components should not require a specific format for the presentation of the countermeasures concept. As a minimum, the countermeasures concept section should be the result of the following analyses for each countermeasure:

a. Why they were selected;

b. When and how they will be implemented or increased;

c. When, how, and why they will be terminated or reduced;

d. How much they are expected to cost; and

e. Any differences in protection levels between facilities owned by the government and by contractors; especially with regard to test facilities and the reasons for the difference. Compliance with the Program Protection Plan will be included in the list of Terms and Certifications and the Statement of Work (SOW) of the government's solicitation.

6. Training in acquisition system protection and security awareness are integral parts of the countermeasures effort.

a. Following the approval of the PPP by the Milestone Decision Authority, PMs should implement a training program to inform all members of their program of the efforts, procedures, and methods to be used to protect the system's EPITS, classified information, and sensitive controlled information.

b. Emphasis should be placed on the encrypted transmission of electronic messages, facsimile transmissions, and telephone transmissions relating to EPITS or sensitive unclassified information.

7. Countermeasures are dynamic with the passage of time. As the threat, EPITS, or environment change, the countermeasures will also change. Although formal updates and validation of the protection plan are only required at each Milestone Review, PMs should update their PPPs as system vulnerabilities change to reduce the cost and administrative burden on their programs.

J. COST

1. Cost data associated with countermeasures and other protection efforts shall be compiled and tabulated as part of the PPP by acquisition phase.

Costs should be differentiated by security disciplines and sub-categories (e.g., physical security, personnel, products, services, and equipment).

2. Cost data for the current phase should be as specific as possible. In addition, the cost data for the previous phase should be compiled and compared with the estimated target. Significant differences between the projected and actual data should be explained.

CHAPTER 4

TIME- OR EVENT-PHASED SECURITY CLASSIFICATION GUIDE

A. GENERAL

1. This chapter is provided as a supplement to the policy provided in DoD 5200.1-R (reference (c)) and DoD 5200.1-H (reference (s)). This chapter provides guidance on the preparation of security classification guides that is unique to the acquisition systems protection process. In the case of a conflict between the requirements of this chapter and those of the cited references, the provisions of the more stringent requirement should apply for activities related to the acquisition systems protection program.

2. Each acquisition program, product, or project that is required to develop a Security Classification Guide in accordance with DoD 5200.1-H (reference (s)) shall develop such a guide that is time- and/or event-phased.

3. The guide should not be finalized until the system's EPITS have been identified as part of the preparation of the program protection planning.

4. For those programs governed by the DoD 5000 series of Directives and Instructions, the guide is necessary to reduce the administrative burden of excessive classification and reduce protection costs.

5. The classification guide should be developed as soon as required, but no later than Milestone I, and made an attachment to the PPP.

B. REQUIREMENTS

1. Although all of the EPITS may not be classified, the guide will focus on the classified elements.

2. Each EPITS should be identified with a statement regarding its releasability to foreign governments, international organizations or their designated representatives. Identify the releasability with one or more of the disclosure categories in DoD Directive 5230.11 (reference (l)). If a substitute technology is known or planned that would allow releasability, identify that technology.

3. Those EPITS that do not meet the criteria of DoD 5200.1-R (reference (c)) for protection at the classified level should be evaluated for protective markings and distribution controls under DoD Directive 5230.24 (reference (t)) and DoD Directive 5230.25 (reference (u)). The guide shall describe how this unclassified, controlled information will be protected.

4. The guide should be reviewed and updated at least every 2 years throughout the system's life cycle.

a. In addition to the biennial reviews, the security classification guide shall also be reviewed prior to each Milestone Review, and updated and validated when necessary.

b. Any changes from previous versions should be compiled in a summary of changes section.

5. Each item listed in the classification guide shall contain specific criteria and guidance on

the elevation, reduction, or declassification of the element. To the maximum extent possible, this guidance should be directly related to specific times or events that can be used to evaluate changes in the classification levels.

C. CLASSIFICATION

1. PMs (and their staffs) must consider three scenarios with respect to the question of security classification. These are:

a. Evaluating information that is similar to that identified as classified in security classification guidance of other programs;

b. Properly identifying as classified that information which is used as such in the current effort; and

c. The potential for an original classification authority needing to decide whether information will be classified.

2. Original classification requires authority delegated in writing in accordance with DoD 5200.1-R (reference (c)). Derivative classification is a responsibility of those security-cleared individuals who use information previously classified.

3. Information that is similar to that identified as classified in similar systems should be considered for classification. Because individual systems may have unique features or be utilized in unique circumstances, differing conclusions may be reached. When a characteristic of one system is classified, careful thought should be given to classification of that characteristic in the system under development. A decision to classify (e.g., design lethality at a given range and altitude) in these circumstances would require original classification authority. Horizontal uniformity of classification determinations is desirable, even necessary, when all relevant considerations are the same.

a. A listing of most security classification guides is published annually in DoD 5200.1-I (reference (v)).

b. Derivative classification responsibility serves as the basis for classifying most existing technology or elements of information common to multiple programs.

b. Original classification authority may be required for some elements of the program. The most likely candidates are those elements that are products of new technology or information. Possible examples of reasons for invoking original classification authority include:

(1) Information that provides U. S. defense operations with a scientific, technical, operational, intelligence, or battlefield advantage.

(2) Indications that disclosure would weaken the international position of the United States.

(3) Indications that disclosure would weaken the country's ability to wage war, limit the effectiveness of forces, or render the United States vulnerable to attack or compromise.

(4) Indications that other nations may not know the United States has, or is capable of obtaining, certain information or material.

(5) The item under development represents a significant breakthrough in research with direct military

application.

(6) There is reason to believe knowledge of the information would:

(a) Allow a foreign nation to develop, improve, or refine a similar item,

(b) Provide a foreign nation with the technical base required to develop counter-measures, or

(c) Weaken or nullify the effectiveness of the system.

D. DECLASSIFICATION AND DOWNGRADING

Declassification criteria and the criteria for reducing the classification level shall be an integral component of the guide. The cost and administrative burden of inappropriate or excessive classification levels shall not be sanctioned by the DoD Components. Possible factors that may be used by program offices to authorize and plan a reduction or elimination of classification include:

1. The occurrence of an anticipated event.

2. The anticipated compromise due to widespread use or dissemination.

3. The expectation of public release.

4. Changes in the international political climate.

5. Changes in emphasis or reliance on a product or tactic.

6. The anticipated correction of a shortcoming or weakness of the system.

CHAPTER 5

TECHNOLOGY ASSESSMENT/CONTROL PLAN

A. GENERAL

1. This chapter is provided as a supplement to the policy provided in DoD Directive 5530.3 (reference (w)). It is not designed to replace nor supersede the policy presented in that Directive. In the event of a conflict in policy between this chapter and reference (w), the policy prescribed in DoD Directive 5530.3 (reference (w) shall apply.

2. A Technology Assessment /Control Plan (TA/CP) has been established as a mandatory requirement for all acquisition programs.

3. The TA/CP is an attachment to the PPP.

B. PURPOSE

The TA/CP shall be used to:

1. Assess the feasibility of the United States' participation in joint programs from a foreign disclosure and technical security perspective.

2. Prepare negotiation guidance on the transfer of classified information and critical technologies involved in the negotiation of international agreements.

3. Identify security arrangements for international programs.

4. Draft the Delegation of Disclosure Authority Letter that provides specific guidance on proposed disclosures.

5. Support the acquisition decision review process.

6. Make decisions on Foreign Military Sales, commercial sales, and co-production or licensed production of the system or international cooperative agreements involving U.S. technology or processes.

7. Make decisions on the extent and timing of foreign involvement in the program, foreign sales, and access to program information by foreign entities.

C. CONTENT

The TA/CP is composed of four sections, the Program Concept, the Nature and Scope of the Effort and the Objectives, the Technology Assessment, and the Control Plan.

1. The first section, Program Concept, requires a concise description of the purpose of the acquisition program. It should describe, in the fewest words possible, the purpose of the system and the threat or the military or technical requirements that created the need for the system. The description must be consistent with the PPP. The pertinent sections of the PPP may be referenced to provide additional details, if necessary.

2. The second section is Nature and Scope of Effort/Objectives. Its purpose is to briefly explain the operational and technical objectives of the program (e.g., co-production, cooperative R&D) and discuss any foreign participation or involvement. This issue may not be considered in the early stages

of the program. If foreign participation or involvement or releases of information to support potential foreign sales are considered likely, the phasing and disclosures at each phase should be described briefly; this issue will be addressed in more detail in section 4 and in the DDL. Points of contact for all aspects of the TA/CP must be identified, including address, telephone numbers, and tele-facsimile numbers.

3. A Technology Assessment is required in the third section. This is the most important part of the TA/CP and preparation will require a joint effort involving program management, security, intelligence, and foreign disclosure personnel.

a. When the TA/CP is prepared in the early stage of program protection planning, emphasis will be placed on describing the value of the technology and systems in terms of military capability, economic competitiveness of the U.S. industrial base, and technology; susceptibility to compromise; foreign availability; and likely damage in the event of compromise.

b. It should draw conclusions regarding the need for protective security measures; the advantages and disadvantages of any foreign participation in the program, in whole or in part; and foreign sales. Concerning the last of these, the assessment must be specific concerning phasing of releases of classified and unclassified information in support of potential foreign involvement and foreign sales. For consideration of cooperative research and development, co-production, or foreign sale at subsequent reviews, the preparer must place a value on the U.S. technical contribution to the program, fully assess the benefits to accrue to the United States and perform a risk-benefit analysis.

c. In all cases, this analysis must result in a conclusion on whether a cooperative program, co-production, or foreign sale will result in clearly defined operational or technological benefits to the United States that are expected to outweigh any damage that might occur if there should be a compromise or unauthorized transfer. Specific reasons must be provided.

d. The analysis must identify and explain any critical capability, information, or technology that must be protected; it may reveal that an adjustment to program phasing is necessary so that critical information is released only when absolutely needed; and it will identify the need for special security requirements that would need to be adopted such as a program-specific security plan to govern international involvement. It should identify any EPITS that cannot be released due to the impact on the system's combat effectiveness. The assessment must evaluate the risk of compromise, based on the capability and intent of the foreign participants or purchaser to protect the information and the susceptibility of the system to compromise.

e. This aspect of the assessment also must discuss any known foreign availability of the information, system, and technology involved, and previous release of the same or similar information, system, or technology to other countries and, when foreign involvement or sales are recommended, to other pa-ticipants.

4. The fourth section, the Control Plan, together with the Technology Assessment in Section 3, is the basis for negotiating guidance on the technical and security aspects of the program and

the development of disclosure guidelines for subsequent sales and foreign participation in the program.

a. The Technology Assessment and Control Plan sections are also the basis ultimately for preparation of the Delegation of Disclosure Authority Letter (DDL).

b. The Technology Assessment must describe actions that are to be taken to protect U.S. interests when foreign involvement or sales are anticipated.

c. Possible actions are withholding of certain information, stringent phasing of releases, the development of special security requirements, and program protection planning. It should also identify any design or engineering changes that may be necessary or desirable to ensure the protection of the program's EPITS.

d. These actions must be specific and meaningful and should address the specific risks, if any, discussed in Section 3 of the TA/CP. References to provisions of the PPP, separate agreement for which the TA/CP is prepared, or DoD Component regulations must be avoided. The Control Plan simply describes how security provisions of an agreement and/or applicable regulations are to be applied to the specific program, agreement, or sale.

5. As part of a recommendation for foreign involvement or disclosure of the program to foreign entities, or requests for authority to conclude an agreement, or a decision to authorize foreign sales, the program office shall prepare the DDL.

a. The DDL shall provide detailed guidance pertaining to the releasability of all elements of the system, technology, or information in question.

b. Until the DDL has been approved by the originating authority and by OUSD(P), personnel from the acquisition program shall neither promise to release nor actually release sensitive information or technology.

c. The DDL shall be reviewed by the program office and the appropriate designated disclosure authority pursuant to DoD Directive 5230.11 (reference (l)) and be issued to ensure that all transfers of equipment or information by the government or U.S. industry personnel comply with the provisions of the TA/CP, DoD Directives 2040.2 (reference (e)), 5230.11 (reference (l)), and 5530.3 (reference (w)), and the appropriate DoD or Component security policies and procedures.

CHAPTER 6

SYSTEMS SECURITY ENGINEERING

A. GENERAL

System Security Engineering (SSE) is required in accordance with DoD Instruction 5000.2, Part 6, Section J. (reference (g)). It is an essential element of acquisition systems protection and is the vehicle for integrating security into the overall systems engineering process.

B. PURPOSE

The purpose of SSE is to eliminate, reduce, or control through engineering and design any characteristics that could result in the deployment of systems with operational security deficiencies.

1. During the system's design phase, SSE should identify, evaluate, and eliminate or contain known or potential system security vulnerabilities at deployment and through demilitarization.

2. SSE should also address possible capture of the system by the enemy on the battlefield.

3. A key difference between SSE and program protection is SSE addresses only those security threats against the system during deployment, operations, and support.

4. SSE involves the integration of security considerations into the systems engineering process to ensure the total system is evaluated for known or potential system vulnerabilities and that the system is cost-effectively designed to reduce the probability and severity of all security vulnerabilities.

5. SSE should be applied to new developments (including off-the-shelf and non-developmental items) and to modifications of existing systems to minimize the operational costs of protecting deployed systems.

C. SYSTEM SECURITY ENGINEERING PLANNING

1. The Systems Engineering Management Plan (SEMP) is a top-level management document that describes system engineering tasks.

2. The System Security Management Plan (SSMP) is a detailed plan outlining how the SSE Manager (SSEM) and the contractors are going to implement SSE.

3. It prescribes how security threat vulnerabilities projected for the operational environment will be "engineered-out" and appropriate countermeasures are "engineered-in" for protection of the weapon system.

4. The SSMP may be included in the SEMP or it may be a separate document.

5. The level of detail in these plans may vary depending on the criticality and complexity of the system.

D. MILITARY STANDARD 1785

MIL-STD-1785 (reference (x)) contains the procedures for contracting for an SSE effort and an SSMP. The format and contents of an SSMP are outlined in the appropriate Data Item Description listed in MIL-STD-1785.

1. Implementation requires contractors to establish an SSMP that identifies operational security vulnerabilities and to take action to eliminate or contain the associated risks based upon the level of risk acceptable to the PM.

2. Contracting Data Item Descriptions (DID) and Contract Data Requirements Lists (CDRL) may be tailored to the system in order to obtain contractor-produced plans or studies satisfying specific program needs.

E. INTERNATIONAL PROGRAMS

The SSE concept includes assessment of any security criteria that currently precludes or will preclude international cooperative and/or foreign military sales programs. Engineering and software alternatives, including export variants, that would permit such programs, should be identified and considered for use, where practical.

CHAPTER 7

STANDARDS FOR SECURITY OPERATIONS AT ACQUISITION FACILITIES

A. GENERAL

1. This chapter identifies minimum standards for DoD-owned and operated facilities, including ranges, laboratories, test beds, program offices, off-site testing locations, and demonstration sites, used to support the acquisition of defense systems throughout the research, development, test, and evaluation phases. It specifically includes all events related to developmental test and evaluation (DT&E); operational test and evaluation (OT&E); live fire testing; combat and tactics development; requirements definition; laboratory experimentation; technology demonstrations; and the logistics support and initial training (system or unit) in preparation of OT&E of acquisition systems.

2. A critical challenge faced by acquisition managers in the development and fielding of combat-effective systems is to deny foreign intelligence services information about the EPITS, as well as information about existing weapon systems with which the systems being acquired will co-operate.

a. The period of greatest vulnerability for most systems, and the period that provides the most opportune lead time for an adversary to exploit the information for countermeasure development or technological advantage, is when the system or its critical components are at government acquisition facilities such as test and evaluation ranges and research and development laboratories.

b. Studies have documented vulnerabilities during testing at these sites and have shown that many U.S. weapon systems are in the test and evaluation phase when foreign countermeasure systems are initiated.

3. While the PPP addresses the overall protection of the program's EPITS, special attention must be devoted to the protection of the EPITS at DoD acquisition facilities. As a result, this chapter establishes the minimum integrated protection features that should be available at each acquisition facility as a part of the acquisition infrastructure. Additional protection provisions to support a specific program should be considered "program unique." The PM should be responsible for budgeting and funding for these items based upon risk management.

4. The development of the minimum protection standards has two goals.

a. The first goal is to establish an integrated, multi-tiered series of protective measures at facilities that will provide a uniform level of protection for programs that use the facility as a part of the acquisition infrastructure.

b. The second goal is to establish a protection baseline that will allow the acquisition facility commander or director to identify deficiencies in the

facility's protection assets or the inability to meet program-specific protection needs for acquisition programs that will use the facility.

5. All facilities should strive to have these minimum protection resources available for all supported ACAT I, II, III, and IV programs. Acquisition facility commanders and directors are responsible for providing a secure environment based upon the threat. A facility point of contact (POC) shall be assigned to advise and assist program officials in the implementation of security procedures and plans to integrate the acquisition program's protection requirements and the facility's security system.

6. The standards discussed in this chapter may serve as minimum guidance for DoD contractors and their facilities. However, contractor security requirements shall be as specified in the contract and the standards set forth in the DoD Industrial Security Manual (ISM), DoD 5220.22-M (reference (r)).

B. MINIMUM PROTECTION REQUIREMENTS

1. The following information and data may be protected at acquisition facilities (unless waived) as dictated by the perceived threat and the vulnerabilities of the acquisition program to compromise:

a. EPITS, as identified in the PPPs prepared by each program office when a vulnerability exists for the EPITS at that facility.

b. Operational characteristics such as Probability of Kill (P_k) and Wartime Reserve Mode (WRM) information for new and existing weapons.

c. Telemetered or data-linked data or information from which EPITS or operational characteristics can be inferred or derived through reverse engineering. This includes data without scale, units of measure, or calibration (i.e., raw data).

d. Information pertaining to schedules of events during which the above information might be vulnerable or available for targeting for unauthorized collection.

e. Communications (telephonic, radio, conversations, written, briefings) and data transfer that can lead to knowledge by unauthorized collectors about the nature or presence of EPITS, P_ks, or WRM in any acquisition event at any acquisition facility.

2. Each acquisition facility commander or director (see DoD Directive 5200.8, reference (y)) should:

a. Ensure that facility protection plans are prepared;

b. Designate a POC at the facility;

c. Establish working groups that will have the primary responsibility for liaison and integrating the supported programs and their protection requirements into the facility protection planning process;

d. Provide listing and descriptions of available countermeasures to protect EPITS while the program is resident at the facility;

e. Implement and employ internal facility security control and auditing procedures;

f. Develop quantitative standards that indicate the

effectiveness of the facility's protection efforts;

g. Comply with provisions of DoD and Component directives addressing sabotage (including integrity and availability of data), inadvertent or unauthorized access, accreditation, and certification of the systems;

h. Identify as early as possible, and provide continuous assessment of threats, vulnerabilities, and risks associated with the facility, as well as environmental factors that contribute to facility vulnerabilities;

i. Conduct periodic reevaluations of protection programs to ensure facility countermeasures are appropriate and sufficient to meet the identified threats;

j. Ensure that facility contracts involving the support of acquisition programs, while they are resident at the facility, contain provisions that will include the protection of both classified and sensitive, unclassified EPITS that are released to industry; and

k. Ensure that facility contracts in support of resident acquisition programs will contain provisions that authorize the government to conduct protection surveys of the contractor's facilities used in support of the acquisition program without incurring additional charges for the government.

C. FACILITY PROTECTION PROCESS

1. The facility POC shall:

a. Prepare and maintain facility protection plans, which identify the minimum integrated protection features of the facility and listings of available countermeasures;

b. Advise and help the program office staff with the analysis and implementation of the portion of the PPP that applies to the facility;

c. Establish liaison with the local CI and law enforcement organizations to determine the status of the local threat to the facility, personnel, and supported programs;

d. As information becomes available, inform the supported program offices of the current threat status, any changes since the last update, and any other information required; and

e. Conduct periodic evaluations (and provide a sanitized copy of the results to supported programs), and prepare a consolidated "lessons learned" document to assist with protection planning.

2. If there is uncertainty as to whether resources identified through the PPP are available, the PM and Component headquarters should identify and explore alternatives to the countermeasures described in the PPP.

D. APPLICABLE PROTECTION CAPABILITY REFERENCES

1. The protection measures for acquisition facilities follow the DoD guidance and instructions contained within the directives that apply to the security and counterintelligence disciplines. The references for this chapter include:

a. Information System Security, see DoD Directive 5200.28, reference (z);

b. Communications Security (COMSEC), see DoD Directive C-5200.5, reference (aa);

c. Compromising Emanations, see DoD Directive C-5200.19, reference (bb);

d. Industrial Security, see DoD 5200.22-R, reference (cc) and DoD 5220.22-M, reference (r);

e. Information Security, see DoD 5200.1-R, reference (c); DoD Directive 5230.24, reference (t); and DoD Directive 5230.25, reference (u);

f. Personnel Security, see DoD 5200.2-R, reference (dd);

g. Physical Security, see DoD 5200.8-R, reference (ee); and

h. Protection during transportation and shipment, see Defense Traffic Management Regulation, reference (ff);

2. The effectiveness and coherence of the application of the security disciplines to the threat facing an acquisition facility are enhanced by the application of counterintelligence analysis and OPSEC planning for the facility. Counterintelligence analysis and OPSEC surveys may help the security planner determine the threat (operational and collection) to the facility, and help identify vulnerabilities for information leaks. The DoD guidance on these topics is provided in:

a. Counterintelligence, see DoD Directive 5240.2, reference (gg); and

b. Operations Security, see DoD Directive 5205.2, reference (hh).

CHAPTER 8

PROGRAM PROTECTION SURVEYS

A. GENERAL

1. The DoD goal is to conduct at least one program protection survey (PPS) on each acquisition program during each phase of the acquisition cycle. As a minimum, the PM shall evaluate the need for a PPS during each phase.

2. Following the review of the PPP by the Milestone Decision Authority (or designated representative), implementation of the plan and the training program, PMs may use the survey process to assess the effectiveness of the established program protection efforts.

B. PURPOSE

The PPS is the DoD activity that responds to the survey requirements of DoD Instruction 5000.2, Part 5, Section F (reference (g)). PPSs are conducted following the establishment of the PPP. The PPS simulates an intelligence collection effort aimed at a specific acquisition program's EPITS at a specific RDT&E facility or other location. It is the primary tool to evaluate and validate the current protection planning methodologies and effort. It is similar to other types of surveys in some of the methods it uses, but it differs significantly in objective and scope.

C. OBJECTIVE

The objectives of the PPS are:

1. To assess awareness of the need to implement the PPP,

2. To assess the overall effectiveness of the PPP at a specific point in the acquisition process,

3. To provide specific indicators of losses of EPITS that have or may have occurred,

4. To provide specific information on how the loss of EPITS did or could have occurred, and

5. To point out needed changes in the program protection plan for the remaining acquisition phases.

D. SURVEY PROCESS

1. The PPS is intended to provide the acquisition PM with information that can be used to modify protection efforts. If the protection is determined to be less than required or indicates a waste in resources, the PM is provided with the information necessary to revise the PPP and the protection methods. This assessment will allow the PM to continue the PPP as written or to restructure the plan to appropriately redirect protection resources, policies and/or activities.

2. The PPS may differ from a true adversarial effort in that simulated collection is accomplished with minimal resources, within a limited time frame, and with the intent of identifying, reducing, or eliminating exploitable vulnerabilities.

3. PPSs are conducted to determine if the previously identified EPITS are being adequately protected during a given phase of the acquisition process. The PPS is specifically designed to

evaluate PPP effectiveness and allow restructure as required. It is focused on specific, valid threat and countermeasures issues. The survey methodology seeks to reproduce the adversary's approach to the facility being assessed, as opposed to examining compliance with security procedures and regulations.

4. The PPS is limited to determining the effectiveness of the protection and countermeasures planned and implemented at a specific facility to protect the EPITS of a selected acquisition program from foreign intelligence collection. The PPS provides the PM with a written report on the effectiveness of the protection measures being applied to the program's EPITS and recommendations to improve protection measures that should eliminate or reduce identified vulnerabilities.

5. The PPS is not an inspection. No grades are awarded nor punitive actions taken as a result of the assessment. To obtain accurate information and be successful, the PPS team depends on positive cooperation and assistance from the program management organization and facility being surveyed.

6. A PM shall coordinate survey visits to contractor facilities with the cognizant DIS office of Industrial Security. Where the protection of classified EPITS will be a subject of inquiry, the cognizant DIS office may be requested to participate as a member of the survey team for the purpose of assessing this specific area.

7. The results of program protection surveys should only be provided to the PM.

8. The unit or organization that conducted the protection survey will provide a sanitized, "lessons learned" document discussing the specific areas of the protection plan's strengths and weaknesses as found by the surveying organization.

a. The sanitized report should be correlated against common trends and/or problems in the acquisition community as found by the surveying organization.

b. This sanitized report should be presented to the PM at the same time as the complete survey report and should be subject to a joint review and revision by the PM and the Team Chief of the surveying organization.

c. The sanitized report should concentrate on those problems with resources, facilities, or training that are generic to the acquisition community.

d. The sanitized report shall be forwarded through appropriate channels to OSD (ODASD(I)/ASPO).

CHAPTER 9

HORIZONTAL PROTECTION

A. GENERAL

The objectives of the horizontal protection activities are to ensure:

1. Cost-effective application of systems protection efforts across a technology area or technology thrust by coordination of requirements among programs using similar technologies.

2. Accurate assessments of progress and periodic measurement of effectiveness of systems protection efforts.

B. HORIZONTAL PROTECTION REQUIREMENTS

The DoD Components shall establish processes and information systems needed to support horizontal protection activities. The DoD Components shall:

1. Review the classification guides of existing programs when developing PPPs to determine sensitivity of similar technologies in use or in development. See the Index of Classification Guides, DoD 5200.1-I (reference (v)).

2. Catalogue, analyze, group and correlate protection requirements within approved PPPs for similar EPITS.

C. HORIZONTAL PROTECTION ASSESSMENTS

1. Assessments may be carried out by the PEO or DoD Component for a technology area, technology thrust, or all cognizant programs. Reviews may include the following subjects:

a. Protection measures planned or provided.

b. Intelligence estimates of competitive acquisition efforts.

c. Reports or investigations of compromises, espionage cases, and other losses.

2. The PEO or DoD Component conducting the assessment shall ensure that appropriate PPPs are modified based on conclusions of the assessments.

3. ASD(C3I) will conduct periodic assessments of the effectiveness of overall systems protection efforts.

D. REPORTING REQUIREMENTS

1. The DoD Components should share decision documents based on horizontal assessments with ASD(C3I) and other DoD Components engaged in similar RDT&E.

2. Loss or theft of EPITS are reported as required in DoD Instruction 5240.4 (reference (p)) through CI channels to ASD(C3I).

APPENDIX A

PROGRAM PROTECTION PLAN EXIT CRITERIA

A. APPLICATION OF THE EXIT CRITERIA

The following criteria are provided to help program officials prepare PPPs: (In addition, the criteria should serve as a guide to officials below the level of the Office of the Secretary of Defense who are responsible for the review of PPPs.)

1. The criteria presented are for a mature system; i.e., an acquisition program at the Milestone II review or later. Accordingly, the scope and depth of the PPP are not expected to be as great for programs earlier in the acquisition cycle.

2. In addition, not all programs will require this level of detail. If a program does not have any EPITS, a conclusion based upon a thorough review of the technology involved and the possible threats to the program, then the PPP may consist of a single sentence stating that fact. As a result, officials reviewing the PPP should use discretion in applying the criteria contained in this section.

B. EXIT CRITERIA

1. Does the summary description of the system:

a. Identify the mission, military value, and expected operational parameters?

b. Identify the locations or facilities where, and time periods when, EPITS will be used, stored, tested, or analyzed?

c. Identify unusual factors (such as Treaty Limited Items) that may serve to increase or decrease foreign intelligence interest in the program?

d. Identify supported or supporting programs?

2. Does the description of the Essential Program Information, Technologies, and/or Systems (EPITS):

a. Identify the technical parameters that, if compromised, would reduce the combat effectiveness or the combat effective lifetime of the system?

b. Establish the criteria for what constitutes "loss" of the information?

c. Identify the EPITS of supporting programs and describe how the loss or compromise of these elements would affect the program?

d. Identify any production or fabrication techniques that are unique to the protected system or element and whose compromise would endanger the established EPITS?

3. Does the threat and vulnerability analysis:

a. Identify which countries or organizations have the interest and capability to collect information about the program?

b. Indicate which other countries are performing research in the area of the program's EPITS, identify the level of sophistication of that research, and identify how well the other countries are protecting their research efforts?

c. Indicate where, when, and under what conditions the EPITS will be vulnerable to compromise or loss due to the identified threat?

4. Does the countermeasures concept:

a. Indicate that it is time- or event-driven in its implementation or termination of the protection measures?

b. Formally commit the PM to a level of protection or a security concept?

c. Deploy assets to counter the recognized vulnerabilities of the program based upon a cost-benefit analysis?

d. Provide justification for the security concept that will guarantee minimum protection?

e. Reflect how supporting and supported programs' EPITS will be protected?

f. Indicate how the program office will measure the effectiveness of the countermeasures concept and indicate a procedure to be followed to update and validate the concept?

5. Does the cost criteria:

a. Provide the cost data by acquisition phase?

b. Separate the funds required into security disciplines and categories (e.g., physical security, personnel, products, services, equipment)?

6. Does the Time- or Event-Phased Security Classification Guide:

a. Correlate with identified EPITS and reflect the protection strategy outlined in the PPP's countermeasures concept?

b. Discuss how the EPITS-related material will be classified or protectively marked to limit distribution and control the information flow to unauthorized activities?

c. Clearly indicate what criteria will be used to determine if the classification level should be reduced or eliminated?

d. Provide a justification of why any indefinite periods of classification must be used?

7. Does the Technology Assessment Control Plan (TA/CP):

a. Describe the system, its mission, and its military value?

b. Indicate which technologies; i.e., EPITS, are critical to the system and why they are valuable to the United States in terms of the technology involved and projected military capability?

c. Describe the specific benefits the United States will gain from international cooperation?

d. Indicate the probability of compromise and the possible damage that might occur to the military capability or the industrial base if the technology (EPITS) is lost?

e. Clearly and thoroughly describe how any technology cleared for foreign programs will be protected or controlled to prevent adverse impact upon the effectiveness of the U.S. weapon systems?

f. Include a Delegation of Disclosure Authority Letter (DDL) that provides clear, explicit guidance on the implementation of any joint ventures?

8. At Milestone II and later, does the System Security Engineering section:

a. Identify the threats and vulnerabilities of the system in the operational environment?

b. Identify the design features that will ensure the most efficient and effective security concept for the system in the operational environment after considering the impact of any design changes on the cost, schedule, or performance of the system?

c. Consider what changes can be made in fielded systems that will allow the system to be exported under foreign cooperative agreements?

d. Outline the methodology for achieving the system security goals by acquisition phase?